

16. Thus, Pacific Bell and the other RBOCs clearly have not thought out how to provision a fraud-resistant Call Forwarding product. They seem not ready to acknowledge this shortcoming, or perhaps simply choose to ignore the issue because they are in a position where they do not bear the consequences of their inadequately protected call forwarding products. It is not reasonable to draw a parallel, as Pacific Bell does,⁷ between call forwarding fraud and IXCs' calling card fraud. There is a fundamental difference: IXCs pay the fraud costs associated with their card fraud, and therefore are motivated to prevent that fraud. But the RBOCs do not pay the fraud costs associated with call forwarding fraud. The IXCs pay twice -- once by carrying fraudulent calls, on which they earn no revenue, and again, in access charges paid to the RBOCs on the fraudulent calls.⁸

⁷ Id. at 59.

⁸ Pacific Bell also comments about a recent "calling card fraud operation" in which an employee at MCI stole calling card numbers from an MCI database, and sold them for fraudulent usage. In raising this irrelevant point about insider fraud, Pacific Bell is attempting to divert the Commission's attention from the much more important issue of technical fraud prevention systems. Insider fraud could happen to any carrier and is a problem that must be addressed by that carrier. Internal fraud is irrelevant to the point that Pacific Bell refuses to take effective steps to prevent fraud by other than insiders, and it is non-insider fraud that accounts for the overwhelming bulk of the fraud costs borne by telecommunications carriers.

Moreover, Pacific Bell's comments are based on a newspaper article that is riddled with misinformation, including such basic facts as the amount involved: The Ivy Lay fraud was responsible for approximately \$27M in losses, not the \$50M quoted in the press article. The quotation from Pacific Bell also says that AT&T, Sprint, and other IXC calling card numbers were stolen. In fact, only MCI and LEC calling cards were involved, because MCI does not carry calls that are to be charged to calling cards

IV.

TFPC Recommendations Are Often Not Implemented by RBOCs

17. Despite the dominant influence of RBOCs in the TFPC process, TFPC occasionally does come up with useful recommendations for RBOC actions to prevent fraud, but those recommendations are then often ignored by the RBOCs, at least until other major pressures force them into action. Guggina's example of Call Forwarding is a good one and provides an example of how RBOCs often use "infeasibility" as an excuse for not implementing needed protections, in spite of the fact that those protection mechanisms are quite feasible. It has been almost three years since the call forwarding issue was brought to the TFPC. But Pacific Bell, according to its Reply Comments,⁹ is still exploring and evaluating the technological and economic feasibility of two of the most important of the TFPC recommendations, which suggested reasonably simple and quite feasible upgrades to Pacific Bell's switching network: limit the number of call forwarding paths, and limit the number of times the call forwarding number can be changed. Pacific Bell had these recommendations early enough that they could have been implemented within a useful time frame. Bellcore listed numerous fraud prevention requirements in its original documentation in 1989. Oddly enough, those Bellcore requirements were provided to the TFPC study group by the MCI representative, not by any of the

issued by other IXCs.

⁹ Pacific Bell Reply Comments at 58.

RBOCs' representatives (who were apparently unaware of this basic product description provided by their contractor). The two recommendations that Pacific Bell says it is now considering¹⁰ were part of the original issue statement that was sponsored by AT&T at the TFPC early in 1993.¹¹ The switch upgrades that would be required to implement these recommendations have been available for some time, and in fact have been implemented by other RBOCs. Pacific Bell, on the other hand, according to its Reply Comments,¹² is still investigating the "feasibility" of those available upgrades.

18. The IXCs have been forced to protest a number of RBOC products that incorporate call-forwarding-like features that are directly responsible for abuse of the IXC networks. The tariffing of these defective products took place during and after the closure of the Call Forwarding issue in the TFPC; so it is clear that the RBOCs were aware of the problem, through their TFPC participation. But that knowledge apparently did not provide enough motivation for the RBOCs to implement fraud-prevention mechanisms associated with their call-forwarding products.

19. This isn't just MCI's observation. Just last year, the staffs of both the Arizona Public Utility Commission and the New

¹⁰ Id.

¹¹ TFPC Issue #26, initiated February 18, 1993.

¹² Pacific Bell Reply Comments at 58.

Mexico State Corporation Commission recommended that US West make major modifications to its initial proposals to tariff a call forwarding service so as to minimize the potential for fraud, and that US West be required to credit IXC's for access charges associated with any fraud that might have been encountered due to the proposed product. The staffs' recommendations are attached hereto as Exhibit A.¹³ In both cases, after the staffs made the recommendations, US West withdrew the tariffs. Many of the proposed modifications were taken directly from the TFPC recommendations, which were themselves based largely on recommendations from the RBOCs' primary technical advisory body -- Bellcore. The original Bellcore recommendation is attached hereto as Exhibit B.¹⁴ As can be seen from a comparison of Exhibits A and B, the staff recommendations are sufficiently close to the original Bellcore recommendations -- the feasibility of which is supported by the fact that they came from Bellcore -- that it could hardly be argued that the staff recommendations were infeasible.

¹³ Memorandum to The Commission from Utilities Division of the Arizona Public Utilities Commission, Re U S West Communications, Inc. - Tariff Filing to Introduce New Custom Calling Features, Docket No. E-1051-94-298, (Arizona PUC April 20, 1995); Direct Testimony of Ken Solomon, Director of the Telecommunications Department of the New Mexico State Corporation Commission in In the Matter of an Application of US West Communications, Inc. to Amend its Exchange and Network Services Tariff to Introduce Remote Access Forwarding and Scheduled Forwarding, Docket No. 95-392-TC (NM Corp. Comm'n. filed Sept. 20, 1995), attached as Exhibit A.

¹⁴ See TR-TSY-000217, Issue 2, November, 1988, entitled "CLASS Feature: Selective Call Forwarding," attached as Exhibit B, especially at 4, 11-13.

20. Another instance of an RBOC's attempt to implement forwarding services without serious consideration of fraud potential occurred recently in Iowa. US West filed a tariff for remote access call forwarding (RACF) and scheduled forwarding (SF). When the long distance carriers became aware of the tariff, the Iowa Utilities Board was very responsive and suspended US West's tariff filing, pending the outcome of the Board's investigation of the tariff. Ultimately, the dispute was settled, with US West agreeing to monitoring measures to facilitate fraud prevention.¹⁵

21. Incidentally, Pacific Bell is correct, in its Reply Comments, in pointing out that the Arizona filing by US West, as well as the call forwarding tariffs that Pacific Bell filed, were related to wholesale and remote-access features, not to the basic call forwarding service itself. But that does not change the fact that it was the fraud potential of those features that caused the Arizona and New Mexico staffs to suggest that US West should implement the processes recommended by TFPC. Those features, as Pacific Bell points out, are not themselves the basic cause of call forwarding fraud -- the basic service itself provides the fraud potential. But both the wholesale service and the remote access feature do give a fraud perpetrator more convenient access

¹⁵ Proposed Decision and Order Granting Joint Motion and Approving Settlement, In re: U S West Communications, Inc., Docket No. RPU-95-5 (TF-95-230) (Iowa Util. Bd. Feb. 23, 1996).

to the basic service that he or she wants to subvert.

V.

RBOCs Have Been Inexcusably Slow To Provide Fraud Prevention Mechanisms, Even When Quick Implementation of Those Mechanisms Has Been Demonstrably Feasible.

22. The speed of implementation of fraud prevention techniques depends greatly on the motivation of the parties concerned. Technology is not the problem: As will be explained, the IXCs moved quickly and effectively, when they had control of the process; the LECs have moved extremely slowly, even when the fraud potentials were pointed out to them in advance of implementation of new systems.

23. After Judge Greene's order mandating premises owner selection for all "0+" interLATA payphone calls,¹⁶ thereby allowing other IXCs to compete with AT&T in the provision of operator services, but prior to the implementation of the RBOCs' line information data base (LIDB), the IXCs were dependent upon independent data base service providers. During the initial entry into these new services, the IXCs experienced significant fraud related to the associated LEC products and billing options (e.g., operator assisted LEC calling card, collect and billed to third party calls). The IXCs worked with the database service providers to develop fraud detections systems and bad number screening databases. In the case of MCI, it designed and

¹⁶ United States v. Western Electric Co., Inc., 698 F. Supp. 348 (D.D.C. 1988).

implemented its operator services system platform within 110 days of Judge Greene's order. In addition, MCI had the database service providers implement fraud monitoring and bad number screening database capabilities within 45 days of initial requests. Clearly, when appropriate incentives exist, such preventive measures can be implemented quickly and effectively, and RBOC claims of infeasibility of implementation are demonstrably incorrect.

24. But when LIDB was implemented, the ability to access the required data and perform the required database functions was removed from the IXCs and transferred to the LECs who controlled LIDB. The IXCs were seriously concerned about the fraud aspects of LIDB long before LIDB was actually implemented, in January 1991. Two years prior to the implementation of LIDB, MCI raised the fraud concern that LIDB would eliminate the valuable traffic monitoring capability that was then being provided by the database service providers. It is fair to say that the RBOCs moved at a snail's pace in addressing MCI's fraud risk concerns. It was not until 1994 that the fraud systems MCI requested were implemented by the majority of the RBOCs, nearly six years after the original request, with at least some RBOCs still in the process of provisioning the capability.

25. It is easy to compare performance based on incentives. It required 45 days days for independent database providers and

110 days for MCI to implement the required systems. But it required nearly six years for RBOCs to do so -- six years during which the RBOCs collected access, B&C (billing and collection) and LIDB fees for fraudulent traffic generated by their poorly implemented products. We are not aware of any technical reasons why the RBOCs could not have implemented the required fraud prevention systems in time periods comparable to the short times within which MCI and independent database providers implemented such systems. But even if there were some excuses for significant delays in implementing fraud-prevention features in LIDB, the RBOCs could have recognized the valid fraud concerns and asked the Commission for an extension of the cut-to-service date for LIDB. There were no legitimate reasons to rush into LIDB once the fraud risks were discovered. But the RBOCs' interest in gathering the new revenues from the LIDB query fees led them to ignore the fraud concerns, and move ahead with LIDB regardless of those concerns. In either case, it is clear that the RBOCs lacked the necessary incentives to address the fraud problems effectively.

VI.

Pacific Bell's Claims of Fraud Prevention Actions
and Recognition Thereof
Are Exaggerated and, in Some Cases, Entirely Incorrect.

26. It is true that MCI presented an award to Pacific Bell's MCI Account Team. However, that award was NOT for Pacific Bell's actions concerning fraud prevention, as Pacific Bell claims in its Reply Comments.¹⁷ Rather, it was for efforts of that Account Team to arrange for Pacific Bell to provide facilities such as dark fiber and SONET rings to MCI. Pacific Bell's claim that MCI has commended it for its fraud prevention efforts is simply wrong.

27. For Pacific Bell to attempt to portray itself as a company that addresses fraud issues with due diligence¹⁸ is a misrepresentation of the facts. Effective incentives for fraud prevention by RBOCs do not exist. If such incentives had existed, the Commission would not have needed to institute its proceeding on toll fraud, which addresses responsibilities for fraud prevention and liability in the telecommunications industry.¹⁹ The fact has been and remains that for every fraud dollar that MCI writes off due to poorly implemented RBOC products, the RBOCs collect access, B&C and LIDB fees, thereby generating undeserved

¹⁷ Pacific Bell Reply Comments at 55.

¹⁸ Id. at 58.

¹⁹ Policies and Rules Concerning Toll Fraud, CC Docket No. 93-292.

revenue. MCI does not have major fraud problems with any of its own proprietary products. The majority of MCI's fraud loss interdiction efforts are focused on damages caused by RBOC services and products.

28. Pacific Bell claims²⁰ that MCI refers other BOCs to Pacific Bell's Centralized Fraud Bureau ("CFB") to learn about fraud prevention techniques. MCI has, indeed, referred other BOCs to Pacific Bell, specifically with reference to Pacific Bell's "Sleuth" system, but not for education about broadly applicable fraud-prevention techniques. MCI hoped to encourage those BOCs to pay more attention to fraud prevention, via use of the Sleuth system. The reason MCI referred other BOCs to Pacific Bell was that Sleuth was the only existing fraud-sensitive system that was compatible with LIDB -- the database system used by many other LECs. But even for those LECs which do use LIDB, Sleuth only addresses a limited range of fraud problems. It monitors the use of LEC calling cards and certain operator-assisted calls, i.e., collect calls and calls that are billed to third parties. It does not address the call-forwarding problem except indirectly, when illegitimately forwarded calls are then used to place calling card or operator assisted calls. The references were not because of any broad-ranging fraud prevention programs within Pacific Bell. In this regard, Pacific Bell is perhaps one of the least

²⁰ Pacific Bell Reply Comments at 55.

ineffective of the RBOCs in addressing fraud problems, but it is far from fully effective.

29. Further in that same paragraph,²¹ Pacific Bell mentions its efforts, through its CFB and "The Alliance to Outfox Phone Fraud," to encourage consumers to help fight telephone fraud. The consumer does have an interest in the control of telefraud. But the consumer is clearly not in a position to create a significant impact on telefraud problems if the products that are being sold to the consumer are riddled with fraud risk factors. And many of the LEC line services and products do indeed include such fraud risk factors.

30. Pacific Bell claims to have done more than other RBOCs to address the fraud issues that revolve around LEC calling cards and operator assisted services²² by saying that its proprietary fraud detection systems -- Sleuth and the Fraud Alert Systems Tracking Database -- have been judged by experts as being "the best in the country." But even if those systems are the best RBOC fraud systems in the country, that is only half the story: the other half is the gap between what Pacific Bell is actually doing to prevent fraud and what it and the other RBOCs should be doing to accomplish that objective.

²¹ Id.

²² Id.

31. That gap is well illustrated both by shortcomings in the list of "potential solutions" that Pacific Bell claims, on page 57 of its Reply Comments, to have implemented, and by Pacific Bell's failure to implement the two recommendations that Pacific Bell mentions on page 58. Pacific Bell is proud of having restricted call forwarding to certain types of numbers -- 0+, 0-, 011, 10XXX, 900, N11, and 976. But it has NOT blocked calls to 950-XXXX and 800/950-XXXX numbers. That failure enables fraudulent callers to make calling-card calls from areas where card-calls to specific locations have been blocked by the card issuer because of high incidence of fraud. The LEC, of course, collects access charges for those fraudulent calls. The items on page 58, which Pacific Bell has not implemented, would also assist in curtailing fraudulent calls. Those switch upgrades would limit the number of calls that could simultaneously be fraudulently forwarded from a particular phone, and would limit the frequency with which the forwarded number from a particular phone could be changed. Further, although Pacific Bell claims to have implemented the SS7 detection program, to our knowledge it has not actually done so except in a few trial locations -- not widely enough so that it could actually be effective in fraud prevention.²³

²³ Id. at 57. A further example, in Pacific Bell's Reply Comments, of drawing inferences not supported by the facts is the implication that one arrest in November of 1994 and six arrests in March of 1995 have led to a decrease in the number of call-forwarding fraud cases. Id. at 58. Based on these limited data, it is quite a stretch to suggest that those arrests have had any significant effect on call-forwarding fraud.

32. To the extent that Pacific Bell has implemented fraud-control processes, the primary motivation for doing so has not actually been the prevention of fraud. Rather, the motivation apparently arises from two primary sources: pressure from other organizations and the effects on Pacific Bell customers of fraud-prevention mechanisms put in place by entities other than Pacific Bell. To wit:

- One influence was the numerous conferences and meetings sponsored by MCI's Carrier Relations and other personnel involved in LEC Billing and Technical Security issues, as well as other IXCs, held to encourage expansion of the Sleuth capabilities to address a more complete range of fraud problems.

- The second influence was complaints from Pacific Bell card holders who were justifiably upset that the Pacific Bell card worked differently depending on which IXC network carried the traffic. Each IXC was forced to block card calls in areas where fraudulent abuse was rampant, because Pacific Bell had not accepted liability for fraud associated with Pacific Bell's calling cards. The IXCs' blocking decisions differed from one IXC to another, depending on their own evaluation of the fraud risks in a given area. If the IXCs were indemnified for those fraud losses, or the losses were minimized by effective fraud control on the part of Pacific

Bell, then the IXCs would not be driven to block RBOC calling card calls, and the performance of the RBOC card product would be improved.

33. The basic point here is that Pacific Bell's anti-fraud efforts have generally been implemented only in response to outside pressures, after the fraud problems that should have been addressed in the initial product design had become major problems to other providers. The problems are typically not addressed in the initial product designs, in spite of pointers and recommendations from those entities that are forced to bear the burden of fraud produced via those products. MCI very much supports the actions of PUCs in rejecting or questioning tariffs in which fraud potentials have not been fully addressed. We hope that such actions will help to motivate RBOCs to address fraud problems in advance, rather than after the fact.

VII.

Final Conclusions

34. The position Pacific Bell has tried to portray does not correspond to the reality of the fraud control processes in TFPC and in the telecommunications industry generally. I have been a member of the TFPC for more than five years, and have personally observed the degree to which RBOCs implement the fraud prevention measures recommended by that body. Further, I have noted that the expertise of at least some RBOC representatives in matters of

fraud responsibility and the effects of fraud on IXCs is questionable. For example, the TFPC co-chair mentioned in the Pacific Bell response²⁴ -- a representative of Pacific Bell -- was not aware of such an elementary point as the fact that IXCs pay access charges to Pacific Bell and the other LECs, until just this year, when it came up in a discussion about an article that addressed the subject. Obviously, that representative was not in a position to understand the nature or the magnitude of fraud costs that would be borne by IXCs because of RBOC products for which IXCs not only receive no revenue, because of fraudulent use of the products, but are also required to pay access charges to RBOCs for the "privilege" of carrying the associated non-revenue traffic!

35. The TFPC recommendations have not been adequately effective in preventing fraud. This is not only because of flawed recommendations, although, as discussed above, some of those recommendations are less than ideal, but also because those recommendations are often not implemented by those companies that are in the best position to effectively address the fraud. Whether consciously or unconsciously, the RBOCs often use TFPC as a mechanism for discussion, rather than action, on fraud-prevention issues.

²⁴ Pacific Bell Reply Comments at 56.

36. MCI attempts to limit the fraud impacts of LEC products by restricting the use of those products when the threat can be recognized. Obviously, MCI would prefer to carry the traffic associated with these LEC products, rather than having to limit their implementation due to excessive fraud risks. But MCI cannot do so in a competitive environment when the LEC products generate so much fraud costs. The major source of fraud loss risk for MCI and the other IXCs is LEC products and line services.

Further Affiant saith not.



David P. Jordan

Subscribed and sworn to before me
this 5th day of March, 1996



Notary Public

MARGARET LAU
NOTARY PUBLIC COMMONWEALTH OF VIRGINIA
My Commission Expires March 31, 1998

EXHIBIT A

M E M O R A N D U M

TO: THE COMMISSION

FROM: Utilities Division

DATE: April 20, 1995

**RE: U S WEST COMMUNICATIONS, INC. - TARIFF FILING TO INTRODUCE
NEW CUSTOM CALLING FEATURES (DOCKET NO. E-1051-94-298)**

On August 24, 1994, U S WEST Communications, Inc. (U S WEST) filed tariff revisions to introduce new Custom Calling features. The Commission initially suspended the filing for 60 days (Decision No. 58791, dated September 21, 1994) and further suspended the filing for an additional 180 days (Decision No. 58833, dated November 2, 1994). The interexchange carriers (IXCs) had expressed concern that the proposed new features could result in increased billed, but uncollected, charges for telephone calls and the suspension period was to allow U S WEST and the IXCs the opportunity to meet and determine if the service could be made acceptable to both.

The proposed new Custom Calling features are Remote Access Forwarding (RAF) and Scheduled Forwarding (SF). Both features permit customers to forward incoming calls to another number. While the programmable call forwarding services that are currently available must be activated and deactivated from the subscriber's own phone, with the services proposed in this filing, customers can activate, deactivate, or change their "forward to" number from any tone dialing phone by dialing a local number and using a subscriber-specific personal identification number (PIN). The local number provides access to an automated system which uses a series of prompts to guide customers to make changes via the phone keypad at any location. With Scheduled Forwarding, subscribers can also preprogram the system and schedule in advance specific times, days and destination numbers to which their incoming calls will forward.

The IXCs are concerned because these services allow customers to activate, deactivate, or change the "forward to" number from any tone dialing phone, not just from the subscriber's phone. According to the IXCs, because of the remote access capability, RAF and SF would be more easily used by third parties to fraudulently access and use subscribers' phone numbers to make unauthorized calls without the knowledge of the customer. Fraudulent calls are an important issue to IXCs because not only do they not get reimbursed for the use of their network on such calls, but also have to pay originating and terminating access to the local exchange carriers for these fraudulent calls on which the IXCs receive no compensation.

THE COMMISSION

April 20, 1995

Page 2

U S WEST, however, believes that the proposed services, which incorporate Advanced Intelligent Network (AIN) capabilities such as enhanced toll fraud screening and call forwarding restrictions, will prevent any significant level of fraud from occurring in conjunction with the proposed services. According to the IXCs, significant fraud has occurred with Remote Access to Call Forwarding (RACF) which is a service offered by other RBOCs and is similar to RAF. U S WEST however, differentiates its proposed services from similar services, like RACF, by pointing out that RACF is a central office based service that does not utilize any of the AIN toll fraud screening capabilities that are built into its proposed RAF and SF services.

On February 9, 1995, U S WEST revised its August 24, 1994, filing. At Staff's request, the proposed tariff was revised to include a list of restricted call forwarding destinations for calls forwarded by RAF or SF. U S WEST has agreed to restrict lines equipped with RAF or SF from forwarding to destinations that have typically been used to complete fraudulent calls. Included in the list of restricted calls are: international calls; 800, 700, 900, 950, or 976 calls; all operator assisted dialing arrangements such as 0+ and 0-; N11 and 555-1212 information calls; third-number billed calls; speed dialed calls. Additionally, no more than four calls per hour would be allowed to be forwarded under this service.

The IXCs have recommended that in addition to the restricted call forwarding destinations proposed in U S WEST's revisions of February 9, 1995, U S WEST prevent the forwarding of calls through RAF and SF to payphones. According to U S WEST, the technical capability to prevent RAF and SF from forwarding calls to payphones does not currently exist, but is being developed and will be available within approximately six (6) months. The IXCs are also concerned that a significant number of fraudulent collect calls may be completed using these services and have requested that U S WEST restrict them also. U S WEST, however, feels that the ability to forward collect calls is an important component of this service and that a large part of fraudulent collect calls are made to pay telephones. Preventing calls from being forwarded to pay telephones, then, would significantly reduce the potential for fraud on collect calls forwarded by RAF or SF.

For each line, business or residence, equipped with Remote Access Forwarding and Scheduled Forwarding, the proposed monthly charges are \$6.95 and \$7.95, respectively. U S WEST proposes to waive the standard \$13.00 installation charge in an area during a 90 day introduction period. In addition, if during the first 60 days from installation, the customer is not satisfied with the

THE COMMISSION
April 20, 1995
Page 3

service, the customer may change to a different call forwarding service at no additional charge or U S WEST will credit the customer's account the amount billed for the service.

Staff has reviewed U S WEST's supporting information and has determined that the proposed rates exceed the costs of providing the services. Staff recommends that the tariff be approved, as revised, on an interim basis for a period of twelve (12) months. Staff is recommending interim approval so that RAF and SF can be offered on a trial basis. The purpose of the trial is to gauge the effect the proposed services have on toll fraud levels.

Staff further recommends the following:

- * That during the trial period, U S WEST provide the IXC's the telephone numbers of subscribers to RAF and SF. Subscribers' telephone numbers would be provided to the IXC's under the terms of a protective agreement. This number information would be used by the IXC's solely for the purpose of identifying suspected toll fraud associated with these services. The IXC's should notify U S WEST if any significant fraud occurs within three (3) working days. Subscribers should be notified that this information is being provided to the IXC's.
- * That U S WEST monitor and collect any information which documents or quantifies RAF or SF fraud such as any customer billing adjustments made because of suspected toll fraud associated with these services. This information will allow U S WEST to identify any RAF and SF fraud that occurs. Also, the information collected can be used at the end of the trial period to quantify the effect these proposed services have had on toll fraud levels during the trial.
- * That U S WEST not be allowed to charge the IXC's for the access charge portion of those RAF and SF calls made during the trial period which were fraudulent. Accordingly, at the end of the trial period U S WEST will credit the IXC's for any access that has been paid in conjunction with a fraudulent RAF or SF call.
- * That ninety (90) days prior to the end of the interim approval period, U S WEST should file for permanent approval of the tariff filing if it so desires. At this time, U S WEST should submit the information it

THE COMMISSION
April 20, 1995
Page 4

collected during the trial concerning instances of toll fraud and any actions it has taken to further minimize fraud.

- * That U S WEST install the capability in its network to prevent call forwarding by RAF and SF to payphones within seven (7) months of the date of this Commission Order. If U S WEST expects that it cannot meet this requirement, Staff further recommends that U S WEST be required to file for an extension of time to meet this requirement on or before October 1, 1995, and if the extension is not requested, or denied, that U S WEST be required to suspend offering the RAF and SF services until the Company has certified to Commission Staff that it can prevent calls forwarded by RAF and SF from reaching pay telephones.
- * That U S WEST inform all subscribers to RAF and SF of the trial period and that permanent approval of the services is not assured.

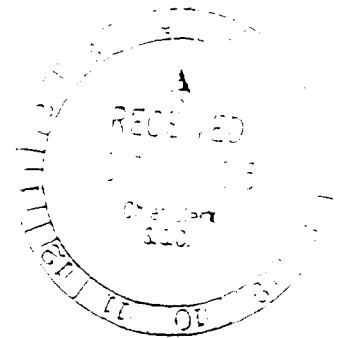


Gary Yaquinto
Director
Utilities Division

GY:DS:lhk/CCR

ORIGINATOR: Del Smith

BEFORE THE
NEW MEXICO STATE CORPORATION COMMISSION



IN THE MATTER OF AN APPLICATION)
OF U S WEST COMMUNICATIONS, INC.)
TO AMEND ITS EXCHANGE AND)
NETWORK SERVICES TARIFF TO)
INTRODUCE REMOTE ACCESS)
FORWARDING AND SCHEDULED)
FORWARDING)

DOCKET NO. 95-392-TC

DIRECT TESTIMONY

of

KEN SOLOMON

Filed September 20, 1995

DIRECT TESTIMONY OF KEN P. SOLOMON

Q. PLEASE STATE YOUR NAME, POSITION AND ADDRESS.

A. My name is Ken Solomon. My position is Director of the Telecommunications Department of the New Mexico State Corporation Commission. My address is: P.O. Drawer 1269, Santa Fe, New Mexico 87504-1269.

Q. DO YOU HAVE A DETAILED STATEMENT OF QUALIFICATIONS AND EXPERIENCES IN THE AREAS OF PUBLIC UTILITY REGULATION?

A. Yes, such a statement is included in Appendix A, attached to this testimony.

Q. IN PREPARING YOUR TESTIMONY WHAT DOCUMENTS AND INFORMATION HAVE YOU REVIEWED?

A. I have reviewed the direct testimony of Ms. Peggy Nownes who filed testimony on behalf U S WEST Communications (the Company), Mr. David Jordan for MCI, Ms. Lilli Calcara for SPRINT and any and all exhibits attached to the aforementioned testimony.

Q. WHAT IS THE PURPOSE OF YOUR TESTIMONY IN THIS PROCEEDING?

A. The purpose of my testimony is to put forth Staff's position regarding the Company's proposal to offer the Remote Access Forwarding (RAF) and Scheduled Forwarding (SF) services.

Q. HAVE SPRINT AND MCI RAISED CONCERNS ABOUT THE POSSIBILITY OF FRAUD ASSOCIATED WITH THESE PRODUCTS?

A. Yes they have.

DIRECT TESTIMONY OF KEN P. SOLOMON

Q. HAS THE COMPANY ADEQUATELY ADDRESSED ALL OF THE CONCERNS
RAISED BY THE INTEREXCHANGE COMPANIES (IXC'S)?

A. No, I do not believe that it has.

Q. COULD YOU PLEASE DISCUSS THE ISSUES SURROUNDING FRAUD IN MORE
DETAIL?

A. Certainly. The Company stated in testimony that the problems raised by the
IXC's associated with third party billing, forwarding to a restricted line and
customer authentication have been solved and that they are unaware of any
toll fraud problems in any of the eight states where the Company currently
provides the service (Nownes Direct, pg. 17, lns 17-20). Yet, the Company
is unwilling to indemnify the IXC's for any toll fraud that may occur (Jordan
Direct, pg. 5, lns. 5-12). In fact, Ms. Calcara claims that in the second quarter
of 1995 alone SPRINT has suffered toll losses in the amount of \$330,000 as a
result of Call Forwarding and RAF/SF in the U S WEST's territory.

Q. COULD YOU PLEASE DISCUSS YOUR RECOMMENDATIONS REGARDING
AUTHENTICATION OF RAF AND SF SERVICE ORDERS WHICH WOULD HELP
TO PREVENT TOLL FRAUD?

A. Yes. In order to authenticate a genuine order for the services in question the
Company could simply take the customers order and then follow this up with
a confirmation letter sent to the billing address associated with that customer.

DIRECT TESTIMONY OF KEN P. SOLOMON

1 Upon receipt of this letter the customer, after reading the literature explaining
2 the service(s) would decide if they still desired the service at which time they
3 would sign the letter and return it to the Company. This procedure would
4 ensure that the individual requesting the service is truly the customer to whom
5 the line is billed. Once the customer has provided written authorization to the
6 Company they would be assigned a PIN number which they could then use to
7 forward call at anytime without any further need for repeat authorization.

8 Q. COULD YOU PLEASE DISCUSS YOUR RECOMMENDATIONS REGARDING
9 CALLS FORWARDED TO A RESTRICTED LINE AND FORWARDED CALLS THAT
10 ARE BILLED TO THIRD PARTIES?

11 A. Yes. USW does not address the issues of the fraud potential inherent in the
12 ability of a "fraudster" to forward calls to a restricted line in its direct
13 testimony. This is a problem on an intra as well as on an interstate basis. The
14 Company does provide a solution for the potential problems associated with
15 intrastate third party billing to a forwarded line but does not provide a solution
16 for interstate third party billing.

17 The Staff therefore recommends that before these services are deployed
18 the Company develop and deploy a method to ensure that calls cannot be
19 forwarded to a restricted line. The Staff further recommends that U S WEST
20 utilize their Line Information Data Base to mark telephone lines that have been